Claims

1. Data exchange method between two devices locally connected to one another, especially between a security module and a receiver, the first device (10) comprising at least one first encrypting key (PAKV) of a pair of asymmetric keys and the second device (11) comprising at least the second encrypting key (PAKB) of said pair of asymmetric keys, these keys being previously initialised in the first and second device, this method including the steps consisting of:
- generating, at least one first random number (A) in the first device (10)
- generating, at least one second random number (B) in the second device (11),
-encrypting said first random number (A) by said first encrypting key (PAKV),
- encrypting said second random number (B) by said second encrypting key (PAKB),
- transmitting said first encrypted random number (A') to the second device (11),
- transmitting said second encrypted random number (B') to the first device (10),
- decrypting, the first encrypted random number (A') in said second device (11)
- decrypting, the second encrypted random number (B') in said first device (10),
- combining said random numbers (A, B) generated by one of the devices (10, 11) and received by the other device to generate a session key (SK),
- and using the session key (SK) to encrypt and decrypt all or part of the exchanged data between the first and second device (10, 11).

2. Data exchange method according to claim 1, characterized in that random number (A), generated with the first device (10) and decrypted with the second device (11)
- is encrypted by said second device (11) by means of said second encrypting key (PAKB),
- is transmitted in a encrypted form to said first device (10),
- is decrypted in this first device (10) by means of the first encrypting key (PAKV) and
- is compared to said random number (A) generated by the first device (10),
and in that the data transfer is stopped if the compared random numbers are not identical.

3. Data exchange method according to claim 1, characterized in that the random number (B), generated by the second device (11) and decrypted by the first device (10)
- is encrypted by said first device (10) by means of said first encrypting key (PAKV),
- is transmitted in a encrypted form to said second device (11),
- is decrypted in this second device (11) by means of the second encrypting key (PAKB) and
- is compared to said random number (B) generated by the second device (11), and in that the data transfer is stopped if the compared random numbers are not identical.

4. Data exchange method according to claim 1, in which said first device (10) and said second device (11) contain a symmetric encrypting key (13), characterized in that the random numbers (A, B) are combined with said symmetric key (13) to generate a session key (SK).

5. Data exchange method according to claim 1 or 4, characterized in that the combination is a concatenation.

6. Data exchange method according to claim 1, characterized in that the session key (SK)is restored in function of a determined parameter of use.

7. Data exchange method according to claim 6, characterized in that the determined parameter of use is the duration of use.

8. Data exchange method according to claim 1, characterized in that at least one of the two devices (10, 11) measures at least one representative physical parameter of the communication, such as the line impedance and/or the electric consumption, in that one compares the values measured to the reference values, and concerning the data exchange when the measured parameters differ from the reference values more than a threshold value.

9. Data exchange method according to claim 8, characterized in that it concerns stopping the data exchange between the two devices (10, 11).

10. Data exchange method according to claims 6 and 8, characterized in that the determined parameter of use is the representative physical parameter of communication.

11. Data exchange method according to claim 1, characterized in that
- at least one of the devices (10, 11) generates at least one supplementary random number (b),
- this supplementary random number (b) is encrypted by said first encrypting key (PAKV)
- this supplementary encrypted random number is transmitted to the second device (11),
- this transmitted encrypted supplementary random number is decrypted in this second device (11),
- the decrypted supplementary random number is encrypted by said second encrypting key (PAKB)
- the supplementary encrypted random number is transmitted to the first device (10)
- the supplementary random number decrypted in the first device is compared to the initial supplementary random number (b) generated in said first device,
- the information exchange is interrupted if the comparison indicates that the two compared numbers are not identical.

12. Data exchange method according to claim 1, characterized in that
- at least one of the devices (10, 11) determines at least one predefined fixed number (c) memorized in the two devices (10, 11),
- this predefined fixed number (c) is encrypted by said first encrypting key (PAKV),
- this predefined fixed encrypted number is transmitted to the second device (11),
- this transmitted encrypted predefined fixed number is decrypted in this second device (11),

- the predefined fixed number decrypted in the second device is compared to the predefined fixed number memorized in this second device,
- the data exchange is interrupted if the comparison indicates that the two compared numbers are not identical.

13. Data exchange method according to claim 11 or 12, characterized in that each of the numbers (A, b, c) is encrypted separately.

14. Data exchange method according to claim 11 or 12, characterized in that a combination of each of the numbers (A, b, c) is encrypted.

15. Receiver for carrying out the method according to any of the claims 1 to 14, this receiver comprising at least one calculation unit, a read-only memory, a demultiplexer, a descrambler, a digital/analogl converter, an external memory and a sound and image descrambler, characterized in that at least the calculation unit, the read-only memory and the descrambler are contained in a same electronic chip and in that at least one of the encrypting keys (PAKB, 13) is stored in said electronic chip.

16. Receiver according to claim 15, characterized in that at least one of the numbers (A, b, c) is stored in said electronic chip.